White Paper zum Datenschutz in der Biometrie

TELETRUST Deutschland e.V.

Arbeitsgruppe Biometrie

Redaktion:
H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock

Stand: 11.03.2008

Impressum

White Paper zum Datenschutz in der Biometrie

Stand 11.03.2008

Verein zur Förderung der Vertrauenswürdigkeit
von Informations- und Kommunikationstechnik

Über TeleTrusT Deutschland e.V.

TeleTrusT Deutschland e.V. hat es sich zur Aufgabe gemacht, vertrauenswürdige und verlässliche Rahmenbedingungen für den Einsatz von Informations- und Kommunikationstechnik zu schaffen. Seit der Gründung 1989 hat sich TeleTrusT zu einem weithin bekannten und geachteten Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa entwickelt. Heute vertritt TeleTrusT Deutschland e.V. mehr als 85 Mitglieder aus der Industrie, Wissenschaft u. Forschung und Behörden. Die Mitglieder finden Gelegenheit, sich in einer Vielzahl von Themen- und Projektgruppen zu aktuellen Fragestellungen der IT-Sicherheit und des Sicherheitsmanagements zu engagieren. Die von TeleTrusT als Projekt betriebene European Bridge CA stellt mittlerweile über 700.000 Public Key Zertifikate der angeschlossenen Teilnehmer für sichere E-Mail Kommunikation im Internet zur Verfügung. Mit dem von TeleTrusT eingeführten T.I.S.P. Zertifikat können sich Experten ihre profunden Kenntnisse zertifizieren lassen.

TeleTrusT Deutschland e.V.
Chausseestraße 17
10115 Berlin

Tel: 030 / 400 54 310
Fax: 030 / 400 54 311
www.teletrust.de

Inhalt

1 Grundlagen

1.1 Was ist das Ziel dieses White Papers?

Dieses White Paper richtet sich insbesondere an Betreiber biometrischer Systeme, deren Ziel es ist, sowohl datenschutzgerechte Lösungen zu installieren als auch die Akzeptanz der Systeme durch die Betroffenen herbeizuführen.

Obwohl an diesem White Paper auch Juristen mitgewirkt haben, kann und will es keine Rechtsberatung leisten. Vielmehr sollen insbesondere Betreiber biometrischer Systeme durch das Aufzeigen potenzieller Gefahren in die Lage versetzt werden, einerseits selbst zu verstehen, worauf es wirklich ankommt und dies andererseits auch den Beteiligten (Daten verarbeitende Stelle sowie Betroffene) zu kommunizieren.

1.2 Was ist Datenschutz?

Aufgabe des Datenschutzes ist es, die Verarbeitung personenbezogener Daten zu regeln. Das vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte Grundrecht auf informationelle Selbstbestimmung schützt "die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Es darf nur durch Rechtsvorschriften eingeschränkt werden.

Aus individueller Perspektive soll der Datenschutz eine Sphäre bewahren, in der sich der Einzelne unbeobachtet und frei von Fremdbestimmung entfalten kann. Informationelle Selbstbestimmung hat aber auch eine gesellschaftliche Funktion: Das Bundesverfassungsgericht hat im Volkszählungsurteil betont, dass "mit dem Recht auf informationelle Selbstbestimmung […] eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar [wären], in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".

Die wichtigsten gesetzlichen Grundlagen des Datenschutzrechts finden sich in der Europäischen Datenschutzrichtlinie, dem Bundesdatenschutzgesetz (BDSG) und den Landesdatenschutzgesetzen. In diesem White Paper wird hinsichtlich der Rechtsgrundlagen nur auf das BDSG verwiesen; je nach Geltungsbereich ist evtl. das jeweilige Landesdatenschutzgesetz zu beachten.

1.3 Welche datenschutzrechtlichen Grundsätze sind relevant?

Das Datenschutzrecht hat eine Reihe allgemeiner Grundsätze, die auch – und gerade – für den Einsatz biometrischer Anwendungen relevant sind. Die wichtigsten sind:

- Die Verwendung personenbezogener Daten ist **nur auf Grundlage einer Einwilligung oder einer Rechtsvorschrift zulässig**. Zu diesen Rechtsvorschriften zählen – wichtig für den Einsatz bei Mitarbeitern – auch Tarifverträge und Betriebsvereinbarungen. Werden die Daten auf Grundlage einer Einwilligung verwendet, so ist diese (mit Wirkung für die Zukunft) widerruflich.
- **Zweckbindung**: Personenbezogene Daten dürfen nur zu vorher definierten Zwecken erhoben werden, und die weitere Verwendung der Daten beschränkt sich auf diese Zwecke. Zweckänderungen bedürfen einer neuen Einwilligung oder Rechtsvorschrift.

- **Erforderlichkeit**: Die Daten dürfen nur in dem Umfang erhoben, verarbeitet und genutzt werden, in dem es zur Erreichung des Verwendungszwecks tatsächlich erforderlich ist. Werden die Daten hierzu nicht mehr benötigt, sind sie (ggf. teilweise) umgehend zu löschen. Im Rahmen der Erforderlichkeit hat die verantwortliche Stelle auch Alternativen zur Verwendung biometrischer Daten zu prüfen (s. den vom Österreichischen Obersten Gerichtshof entschiedenen Fall).

- **Verhältnismäßigkeit** (im engeren Sinne): In bestimmten Fällen ist zwischen den legitimen Interessen an der Datenverwendung (z. B. Zugangskontrollen durch Arbeitgeber, finanzielle Einsparmöglichkeiten) und den Risiken für die Betroffenen (z. B. besonders sensible Daten, insbesondere über die Gesundheit) abzuwägen. Praktisch bedeutet dies, dass in Anwendungen, die kein hohes Sicherheitsbedürfnis erfüllen müssen (Komfortanwendungen, zum Beispiel Thermalbad Mondorf, Luxemburg), Abstriche beim Datenschutz nicht hingenommen werden können.

- **Transparenz und Grundsatz der Direkterhebung**: Die betroffene Person hat das Recht zu wissen, welche Daten über sie zu welchen Zwecken erhoben werden und was im weiteren mit den Daten geschieht; dazu gehört auch das Prinzip, dass die Daten im Grundsatz nicht bei Dritten erhoben werden dürfen. Ausnahmen von diesen Grundsätzen bedürfen einer gesetzlichen Grundlage.

- **Rechte der Betroffenen**: Die Betroffenen haben die Rechte auf Auskunft, Benachrichtigung, Berichtigung, Sperrung und Löschung. Diese können gemäß § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

- **Datenvermeidung und Datensparsamkeit**: Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht (§ 3a BDSG).

- **Schutz sensibler Daten**: „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“ (§ 3 Abs. 9 BDSG) genießen besonderen Schutz. Eine Einwilligung muss sich ausdrücklich auch auf diese Daten beziehen (§ 4a Abs. 3 BDSG), in bestimmten Fällen ist eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG), die Verwendung ist nur in besonderen Fällen zulässig (§§ 13 Abs. 2, 14 Abs. 5 und 6, 16 Abs. 1 Nr. 2, 28 Abs. 6 bis 9 BDSG).

- **Technische und organisatorische Maßnahmen**: Verantwortliche Stellen haben nach § 9 BDSG die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung des BDSG und der Anlage zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.4 Wer ist für den Datenschutz verantwortlich/zuständig?

Für die **Einhaltung** der Datenschutzbestimmungen ist die Daten verarbeitende Stelle verantwortlich, d. h. "jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“ (§ 3 Abs. 7 BDSG).

Für die **Kontrolle** der Einhaltung ist die jeweilige Aufsichtsbehörde zuständig. An diese kann sich der/die Betroffene wenden, wenn er/sie annimmt, in seinem/ihrem Recht auf informationelle Selbstbestimmung verletzt worden zu sein.

1.5 Welche datenschutzrelevanten Anwendungsgebiete gibt es?

Von den rechtlichen Implikationen und den Missbrauchsmöglichkeiten nichthoheitlicher Anwendungen her bietet sich eine Einteilung biometrischer Anwendungen in drei Hauptbereiche an:

Biometrie für Mitarbeiter

Firmen benutzen vielfach biometrische Authentifikationssysteme für den Zugang zu Räumen, Computern, Netzen und Diensten. Auf diese Weise ist ein kostensparendes Rechtemanagement möglich. Die Nutzung durch den Mitarbeiter kann obligatorisch sein, Ausweichlösungen sind aber möglich und nötig.

Biometrie für Kunden

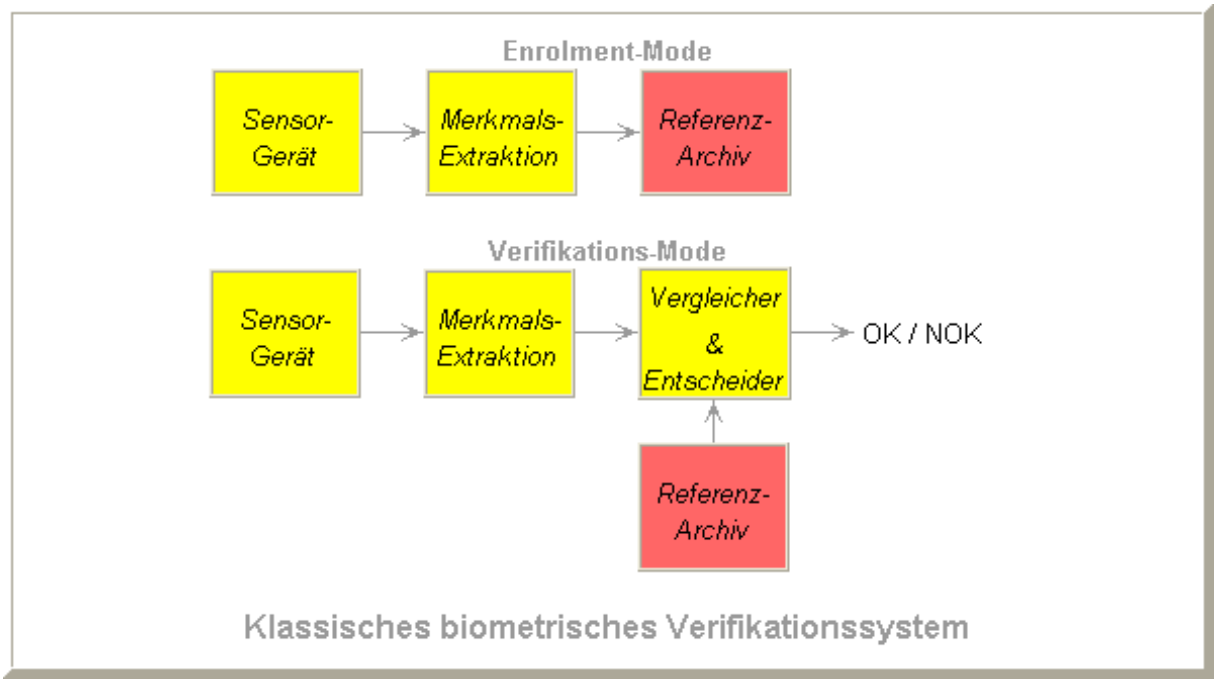
Unternehmen aller Art bieten ihren Kunden immer häufiger Dienste auf der Basis biometrischer Kunden-Authentisierung an. Beispiele sind nicht übertragbare Jahreskarten oder Abonnements für Konzerte, Fitnessstudios, Solarien, Zoos, Bäder, Videotheken, Bezahlsysteme usw.

Biometrie für persönliche Anwendungen

Hierunter fallen Anwendungen, die der vollständigen Kontrolle des Betroffenen unterliegen. Beispiele sind der heimische PC-Zugang, der Wohnungszugang oder die Anwendung im eigenen Auto.

1.6 Welchen Einfluss hat die Systemarchitektur auf die Missbrauchsmöglichkeiten?

Abhängig davon, wo die Referenzdaten der Betroffenen gespeichert sind, können sich erhebliche Unterschiede in Bezug auf Sicherheit, Datenschutz, Administrationskosten, Enrolmentaufwand und Performanz ergeben. Ein biometrisches System (siehe Blockschema) besteht aus einzelnen Funktionsblöcken, die sich relativ gut separieren lassen und somit über wohldefinierte Schnittstellen verfügen.



Damit ist es auch möglich, diese Blöcke an unterschiedlichen Orten zu betreiben, wobei die Gesamtfunktionsfähigkeit über die dazwischenliegenden Verbindungen gewährleistet ist. Diese Verbindungen können geräteintern sein oder über öffentliche oder private Netze führen. Sie lassen sich bei Bedarf mit bekannten kryptografischen Methoden schützen.

Aus datenschutztechnischer Sicht ist besonders das Referenzarchiv von Bedeutung, da hier die persönlichen Nutzerdaten langfristig bis zu einer eventuellen Löschung gespeichert sind, während die biometrischen Daten in den anderen Blöcken und auf den Verbindungen nur temporär während des Erkennungsvorgangs auftreten. Für den Betroffenen ist besonders interessant, wie gut seine persönlichen Daten gegen Fremdzugriff geschützt sind und welche Rechte und Einflussmöglichkeiten er selbst bezüglich seiner Daten hat.

Hat das biometrische System mit mehr als einem Betroffenen zu tun, sind folgende Varianten möglich:

- Das Referenzarchiv enthält die Daten von mehr als einem Betroffenen (Zentralarchiv). Beispiel: Zutrittskontrollsystem oder biometrischer PC-Zugang bei mehreren Nutzern.
- Das Referenzarchiv ist so aufgeteilt, dass jeder Betroffene über sein eigenes Unterarchiv verfügt. Das Unterarchiv ist nur dann mit dem System verbunden, wenn eine Authentifikation erfolgt. Beispiel: Jeder Betroffene verfügt über eine Chipkarte, auf der seine biometrischen Daten gespeichert sind. Diese Daten lassen sich bei Bedarf vom System auslesen.
- Die Blöcke Sensorgerät, Merkmalsextrahierer, Vergleicher & Entscheider und Referenzarchiv sind für jeden Betroffenen dupliziert und unterliegen dem Verfügungsbereich des Betroffenen. Das Referenzarchiv enthält jeweils nur die Daten des Betroffenen. Beispiel: "System on Card" oder Homebankinglösung mit biometrischem Zugang, die komplett auf dem eigenen PC des Betroffenen abläuft.

- Die Blöcke Sensorgerät und Merkmalsextrahierer sind für jeden Betroffenen dupliziert und unterliegen dem Verfügungsbereich des jeweiligen Betroffenen. Die Blöcke Vergleicher & Entscheider und Referenzarchiv sind beim Betreiber der Anwendung lokalisiert. Zum Beispiel: PC-Homebanking mit Datenaufnahme und -kompression beim Betroffenen und zentralem biometrischen Vergleich beim Betreiber.

Untersucht man die angeführten Varianten etwas näher, wird deutlich, dass die Einteilung in zentrales und dezentrales Referenzdatenarchiv keine vollständige Beschreibung der datenschutztechnischen Sachlage ermöglicht. So verschwimmen die Unterschiede zwischen zentraler (alle Daten an einem Ort) und dezentraler Speicherung (verschiedene Daten an verschiedenen Orten), wenn eine permanente Kommunikationsverbindung zwischen allen Datenorten besteht. Es müssen vielmehr weitere Kriterien hinzukommen. Das wichtigste Kriterium dürfte hierbei sein, inwieweit der Betroffene die Kontrolle über seine eigenen Daten ausüben, den Zugriff auf sie kontrollieren und sie löschen kann. Ob dieses Kriterium erfüllt werden kann, ist nicht unmittelbar vom Speicherort abhängig.

Im Folgenden werden drei häufige Fälle zur Speicherung biometrischer Daten betrachtet:

- Dezentrales / mobiles Archiv unter der Kontrolle des Betroffenen
- Zentrales Archiv mit Referenzdaten unter der Kontrolle des Betreibers
- Zentrales Archiv mit Referenzdaten unter der Kontrolle der Betroffenen

1.6.1 Dezentrales / mobiles Archiv unter der Kontrolle des Betroffenen

Bei lokaler biometrischer Authentifikation des Betroffenen, z. B. auf seinem PC, liegen in der Regel auch alle biometrischen Daten in seiner Verfügungsgewalt. Zugriff auf die biometrischen Daten besteht dann nur für die Nutzer dieses PCs bzw. Clients. Somit sind biometrische Manipulationen ebenfalls nur lokal durchführbar und erfordern entweder den physikalischen Zugriff auf den PC oder eine über das Kommunikationsnetz eingeschleuste Schadsoftware. Anmeldungen an netzbasierten Anwendungen erfolgen über die übliche (auswechselbare) eindeutige Kennung/ID.

Beim Wechsel des Arbeitsplatzrechners ist allerdings ein neues Enrolment erforderlich. Zentrale Schutzmaßnahmen gegen biometrische Angriffe sind nur beschränkt möglich. Auch lassen sich bei manchen Systemen die biometrischen Daten der Mitbenutzer nur unzulänglich schützen. Ein Derolment ist ebenfalls nur lokal durchführbar und damit eventuell recht umständlich.

Abhilfe schafft hier das mobile Archiv auf einem geeigneten Token (Smartcard, USB-Stick, etc.), der benutzerspezifisch ist, sich ohne neues Enrolment auf weiteren Rechnern einsetzen lässt und vor allem einen recht guten Schutz gegen den Identitätsdiebstahl bieten kann. Es sind zentrale Schutzmaßnahmen gegen korrumpierte Token (Sperrung wie bei Kreditkarten) möglich, ohne das Benutzer-Konto selbst zu deaktivieren.

Findet der Vergleich der biometrischen Daten in einem Token statt, lassen sich die biometrischen Referenzdaten unauslesbar auf einem Krypto-Chip speichern und verarbeiten. Da der Merkmalsvergleich im Krypto-Chip stattfindet, müssen die Refe-

renzdaten den Token nie verlassen. Dies bietet einen hohen Schutz gegen Brute-Force-Attacken, weil man die Zahl der erfolglosen Vergleiche beschränken kann.

Allerdings muss der Betroffene der Applikation vertrauen, wenn diese das biometrische Charakteristikum außerhalb des Tokens erfasst und in ein passendes Templateformat für den Vergleich im Token umwandelt. Da die Karte eine erfolgreiche Erkennung zurückmeldet, kennt die Applikation damit auch kurzzeitig die biometrischen Daten des Betroffenen, denn eine erfolgreiche Erkennung bedeutet, dass die von der Anwendung erfassten Daten mit den auf der Karte gespeicherten hochgradig übereinstimmen.

Deutlich wird der Vorteil eines Vergleichs im Krypto-Chip bei Anwendung in einem Handy. Hier findet der Vergleich wie bei der PIN in der SIM-Karte statt. Die biometrischen Daten sind nicht auf der relativ offenen Handy-Plattform zu finden und können deshalb auch nicht von anderen genutzt werden, wenn man das Handy verliert. Während des kritischen Authentifikationsvorgangs mit dem Berechtigten befindet sich das Handy zwangsläufig im vollständigen Einflussbereich des Berechtigten. Allerdings ist ein evtl. unbemerkter Identitätsdiebstahl nach wie vor mit Hilfe von Schadsoftware durchführbar.

Unter dem Gesichtspunkt der informationellen Selbstbestimmung sind Lösungen als optimal einzustufen, bei denen die gespeicherten Referenzdaten unter der alleinigen Kontrolle der Betroffenen stehen und ausschließlich zum Vergleich verarbeitet werden. Dies gilt zumindest, sofern der Betreiber des biometrischen Systems die Daten nicht im Verarbeitungsprozess oder direkt vom Sensor abzweigt und eigene Archive unter seiner Kontrolle anlegt. Hier können zertifizierte Komponenten einerseits und vertrauensbildende Maßnahmen durch die Betreiber andererseits den Betroffenen helfen.

1.6.2 Zentrales Archiv mit Referenzdaten unter der Kontrolle des Betreibers

In bestimmten Anwendungen, z. B. Sprecher-Erkennung in telefonischen Auskunftsdiensten, kann ein Zentralarchiv unvermeidlich sein.

Eine Client-Server-Lösung mit zentralem Referenzdatenarchiv und zentralem Merkmalsvergleicher erfordert einen wesentlich besseren Schutz der biometrischen Daten als das lokale Archiv auf dem PC, da die Daten zahlreicher Betroffener hier gespeichert sind. Allerdings lassen sich an zentraler Stelle wirksamere Schutzmaßnahmen in der Regel auch leichter durchführen und überwachen. Beim Wechsel eines Arbeitsplatzes mit biometrischer Authentifikation ist kein neues Enrolment erforderlich.

Sollte der zentrale Schutz allerdings versagen, ist auch mit entsprechend größeren Schäden zu rechnen. Hinzu kommt, dass Angriffe mit biometrischen Fälschungen von überall her initiiert werden können. Auch sind die Benutzerdaten dem Zugriff der berechtigten Benutzer üblicherweise entzogen, so dass diese nicht unmittelbar auf einen Missbrauch reagieren können.

Das Zentralarchiv setzt besonderes Vertrauen in den Betreiber voraus. Denn wenn der Missbrauch vom Betreiber ausgeht, gibt es für die Geschädigten keine Schutzmöglichkeiten mehr.

Datenschutzbehörden sehen europaweit zentrale und vernetzte dezentrale Archive unter Kontrolle der Systembetreiber mit großer Skepsis. Vernetzte dezentrale Archive werfen die gleichen Probleme auf wie zentrale Archive und werden deshalb aus da-

tenschutzrechtlicher Sicht diesen gleichgesetzt, wenn der Zugriff durch den Betreiber funktional betrachtet unter denselben Voraussetzungen und mit denselben Einschränkungen möglich ist.

Gerade größere Archive bergen die Risiken internen Missbrauchs durch den Systembetreiber oder durch zugriffsberechtigte Personen. Außerdem erhöhen derartige Archive den Anreiz für externe Angriffe, weil große Mengen sensibler Daten gespeichert werden. Es gibt eine Reihe von Fallentscheidungen, in denen Datenschutzbehörden aus europäischen Nachbarländern biometrische Systeme mit zentralen Archiven unter Kontrolle des Systembetreibers vor allem bei Behörden, aber auch in der Privatwirtschaft wegen Unverhältnismäßigkeit untersagt haben (Beispiele aus Griechenland, Österreich, der Schweiz, Luxemburg und Belgien). In Deutschland gibt es nur wenige Entscheidungen zu biometrischen Systemen. Beim Reisepass – der als hoheitliche Anwendung in diesem White Paper ansonsten außer Betracht bleibt – wurde jedoch auf jede Speicherung (d. h. sowohl zentral als auch dezentral) der Fingerabdrücke außerhalb des Reisepasses ausdrücklich verzichtet.

1.6.3 Zentrales Archiv mit Referenzdaten unter der Kontrolle der Betroffenen

Eine sowohl sicherheits- und datenschutztechnisch als auch von der Leistungsfähigkeit her besonders vorteilhafte Lösung ergibt sich bei exklusiver Speicherung eines Betroffenen-spezifischen Schlüssels auf einem Token. Mit diesem Schlüssel erfolgt im Falle einer Transaktion die individuelle Ver- und Entschlüsselung der biometrischen Daten im Zentralarchiv. Eine Entschlüsselung erfolgt nur temporär bei Anwesenheit des Betroffenen zum Zwecke des Vergleichs.

Da der Schlüssel ausschließlich auf dem Token gespeichert ist, sind die Merkmalsdaten im Fall der Systemkorrumpierung sicher geschützt. Geht der Token verloren, sind die zentralen Merkmalsdaten ebenfalls unbrauchbar. Bei der Ausgabe eines neuen Token mit neuem Schlüssel erfolgt ein erneutes Enrolment.

Allerdings setzt auch dieses System Vertrauen in den Betreiber voraus, da dieser ja heimlich die Schlüssel dauerhaft im System oder die Merkmalsdaten parallel unverschlüsselt speichern könnte. (Dies ist vergleichbar mit dem Vertrauen, dass der Betreiber eines Geldautomaten nicht heimlich die eingegebenen PINs speichert und für betrügerische Transaktionen nutzt.)

Aus datenschutzrechtlicher Sicht ist diese Lösung ähnlich positiv zu bewerten, wie die Speicherung der Referenzdaten in einem dezentralen Archiv unter Kontrolle des Betroffenen - sofern der Betreiber des biometrischen Systems die Daten nicht im Verarbeitungsprozess oder direkt vom Sensor abzweigt und eigene Archive unter seiner Kontrolle anlegt. Entscheidend für diese positive Bewertung ist, dass auch in diesem Falle der Betroffene bei korrektem Betrieb des biometrischen Systems die Kontrolle über den Zugriff auf seine Referenzdaten hat. Für diese Archivkonstellation bestehen auch die gleichen Risiken wie die beim dezentralen Archiv genannten.

2 Gefährdungen

2.1 Welche biometriespezifischen Risiken für das Recht auf Informationelle Selbstbestimmung gibt es für die betroffenen Personen?

Da biometrische Daten eindeutig und potenziell lebenslang mit dem Betroffenen verbunden sind, eignen sie sich in besonderem Maße zur kontinuierlichen Beobachtung („tracking“) und Datensammlung. Außerdem sind bestimmte Arten biometrischer Daten in besonderem Maße sensibel, weil sie Zusatzinformationen enthalten können. Wie ein Missbrauch konkret aussehen kann, hängt von der Art der verwendeten Daten und der konkreten Anwendung und ihrem Umfeld ab. Schon das unbefugte Sammeln von biometrischen Daten (Fingerabdrücke an Alltagsgegenständen, heimliches Aufnehmen biometrisch verwertbarer Gesichtsbilder) verstößt gegen § 4 Abs. 1 BDSG und ist deshalb als Missbrauch zu qualifizieren.

Für die Betroffenen ergeben sich insbesondere folgende Risiken:

- Identitätsdiebstahl
- Auswertung vertraulicher Zusatzinformationen in biometrischen Daten
- Verknüpfung biometrischer mit anderen personenbezogenen Daten und Bildung von Profilen
- Verletzung der informationellen Selbstbestimmung durch Zwang zur Nutzung biometrischer Systeme
- Überwachung unter Nutzung biometrischer Systeme

Diese Risiken werden im folgenden Abschnitt (2.1.1) zunächst diskutiert und im übernächsten Abschnitt (2.1.2.) durch einige Szenarien und Beispiele verdeutlicht werden:

- Einkauf unter Nutzung des Fingerabdrucks
- Überwachung von Personen mittels Videokameras
- Missbrauch von Zusatzinformationen in biometrischen Daten

2.1.1 Risiken

2.1.1.1 Identitätsdiebstahl

Da biometrische Charakteristika in der Regel keine perfekt schützbaren Geheimnisse sind, lassen sich analoge oder digitale Repräsentationen (z. B. Fingerabdruck-Bilder) als Datensatz kopieren. Damit kann eine der Quelle ähnliche Kopie physikalisch nachgebildet oder verhaltensmäßig nachahmt werden. Der Missbrauch beginnt mit der nichtautorisierten Nutzung fremder Charakteristika beispielsweise zum Zwecke der Bereicherung auf Kosten des Betroffenen. Dazu ist Voraussetzung, dass eine eventuelle Fälschungserkennung (die ein tatsächliches biometrisches Charakteristikum von einem Plagiat unterscheiden kann) überwunden wird. Gefährlich sind in diesem Fall Anwendungen, die im Vergleich zum erforderlichen Angriffsaufwand zu hohe Werte schützen sollen. Identitätsmissbrauch setzt zwei Dinge voraus:
1. Der Missbraucher hat eine digitale oder mechanische Kopie eines biometrischen Charakteristikums erstellt.

2. Das biometrische Zielsystem, auf dem der Missbrauch stattfinden soll, erkennt nicht, dass es sich beim Charakteristikum oder Sample um eine Kopie handelt.
Eine viel diskutierte Methode, einen Identitätsdiebstahl auszuführen nutzt die offen zugänglichen Teile des biometrischen Systems: die Sensoren. Dabei werden dem Sensor Kopien der Charakteristika, so genannte Plagiate, präsentiert. Beispiele für Plagiate sind der Einsatz von Gummifingern oder Dünnschichtkopien von Fingerabdrücken bei Fingerabdrucksensoren (siehe z. B. FIDIS-Studie D.6.1). Wenn das System über keine effektive Methode zur Erkennung von Charakteristikumskopien verfügt, können diese Kopien akzeptiert werden, das System erkennt scheinbar den Betroffenen. Diesen Vorgang bezeichnet man auch als Spoofing.

Es gibt verschiedene Methoden, sich biometrische Daten Dritter bzw. Kopien davon zu beschaffen. So lassen sich unbeabsichtigt hinterlassene latente Spuren biometrischer Charakteristika (möglich z. B. bei DNA, Fingerprint, statischer Unterschrift) direkt kopieren. Das gleiche gilt für öffentliche Bildaufnahmen (Gesicht, mit Einschränkungen auch Iris) und digitale Daten, die durch unberechtigten Systemzugriff entwendet wurden. Voraussetzung ist immer, dass die Spuren eindeutig einer betroffenen Person zugeordnet werden können. Das Zuordnungsproblem entsteht nicht, wenn es gelingt, die biometrischen Daten während der Datenaufnahme des Erkennungsprozesses zusammen mit allen nichtbiometrischen Personendaten abzuzweigen. Besonders gefährdet sind biometrische Systeme, die sich lediglich auf ein biometrisches Charakteristikum stützen und bei denen weite Teile der technischen Infrastruktur öffentlich zugänglich sind und nicht überwacht werden. Eine Übersicht möglicher Angriffswege kann dem Dokument "Biometrics Evaluation Methodology 1.0 (BEM)" entnommen werden.

Eine weitere Methode des Identitätsdiebstahls besteht darin, bei einem Identifikationssystem mit hoher Zahl von Referenzdaten auf gut Glück mit mechanischen Kopien (Plagiaten) eines unbekannten Charakteristikums eine Identifikation zu versuchen. Ist eine Abbildung des unbekannten Charakteristikums tatsächlich im Referenzdatenarchiv vorhanden und wird die Fälschungserkennung überwunden, dann ist damit das Charakteristikum korrumpiert, wenn das System jetzt auch noch den Namen des Betroffenen preisgibt. Dies kann dann sogar Rückwirkungen auf andere biometrische Applikationen haben.

Missbrauchsmöglichkeiten sind anwendungsübergreifend. So kann die Kopie des Fingerabdrucks zur Täuschung der Fingerabdruckerkennung unterschiedlicher Anwendungen herangezogen werden. Dies kann z. B. im Arbeitsumfeld von biometriegestützten Zeiterfassungssystemen über den erschlichenen Rechnerzugang bis hin zum unberechtigten Zugang zu Sicherheitsbereichen reichen.

Die Möglichkeiten des Identitätsdiebstahls sind nicht auf den Fingerabdruck beschränkt. Auch bei der Gesichtserkennung ist z. B. durch Ähnlichkeiten und systembedingte Falscherkennungen der Missbrauch möglich.

Aus Sicht des Datenschutzes sind insbesondere die Betroffenen vor den Folgen eines Identitätsdiebstahls (z. B. einer mechanischen Charakteristikumskopie) zu schützen. Anders als der Betreiber hat der Betroffene nämlich nicht die Möglichkeit, das biometrische System und damit sich selbst gegen die Anwendung von Charakteristikumskopien zu schützen.

Wer im Fall eines Identitätsdiebstahls der Geschädigte ist, hängt von der Anwendung und von den rechtlichen/vertraglichen Bedingungen ab. Dazu einige Beispiele:

- Bei einer biometrischen Arbeitszeiterfassung ist im Fall des "Identitätsdiebstahls" der Arbeitgeber der Geschädigte, wenn der Betroffene sein Charakteristikum als Kopie an einen Kollegen zwecks Vortäuschung seiner Anwesenheit weitergibt. Der Arbeitgeber als Betreiber wird deshalb bestrebt sein, eine dem Risiko angemessene technische Abwehr gegen solche Kopien zu gewährleisten.

- Bei einer Dauerkarte für eine Dienstleistung möchte der Betreiber die Weitergabe durch Einsatz von Biometrie verhindern. Im Falle des Identitätsdiebstahls ist wiederum der Betreiber der Geschädigte, nicht der Betroffene.

- Im Fall von logischen oder physikalischen Zugangskontrollen jeder Art ist der Betroffene immer dann der Geschädigte, wenn der Vortäuschende rechtlich oder tatsächlich erhebliche Handlungen vornimmt, die aufgrund der Täuschung auf den Betroffenen zurückfallen (z. B. bei Nicht-Abstreitbarkeit von Transaktionen).

- Im Fall einer Altersüberprüfung ist bei einem Identitätsdiebstahl weder der Betreiber noch der volljährige Betroffene der Geschädigte, sondern der minderjährige Identitätsdieb. In diesem Fall wird der Gesetzgeber das größte Interesse daran haben, dass ausreichende Schutzvorkehrungen durch den Betreiber getroffen werden.

- Wird Biometrie zum Bezahlen genutzt, ist im Fall des Identitätsdiebstahls zunächst der Betroffene geschädigt. Hier taucht im Weiteren das Problem auf, dass der Geschädigte den Identitätsdiebstahl in der Regel nur schwer nachweisen kann. Das erschwert auch kulante oder kundenfreundliche Regelungen von Seiten des Betreibers. Da Charakteristikumskopien nicht zu verhindern sind, ist vom Betreiber ein besonderer Schutz gegen den Einsatz solcher Kopien zu fordern.

Anmerkung: *Für einen Identitätsdiebstahl per Datensatzkopie stellen Templates, aus denen sich die Originaldaten zurück ermitteln lassen, keinen wirksamen Schutz dar. Selbst verschlüsselte Daten können missbraucht werden, wenn andere Systeme mit dem gleichen Schlüssel arbeiten und der gestohlene Datensatz auf diesem System lauffähig ist. Allerdings sind die praktischen Missbrauchsmöglichkeiten je nach System unterschiedlich.*

2.1.1.2 Auswertung vertraulicher Zusatzinformationen

Manche biometrischen Daten enthalten Zusatzinformationen, die aus Sicht der Betroffenen vertraulich sein können. Zusatzinformationen könnten sein:

- Krankheiten und Krankheitsdispositionen (s. Fidis-Studie)
- psychische Verfassung
- Geschlecht
- Körpergröße
- Rasse
- Vererbungen
- Verwandtschaftsverhältnisse
- etc.

Das generelle Problem bei der Präsentation biometrischer Charakteristika an fremden Systemen ist, dass die betroffene Person (der Träger der biometrischen Charakteristika, der sich authentisieren möchte) diesen Systemen vertrauen muss. So muss er dem Betreiber glauben, dass keine über die Identifikation hinausgehende unerwünschte Auswertung von Zusatzinformationen erfolgt. Am besten ist es, wenn das zur Identifikation benutzte Charakteristikum solche Zusatzinformationen gar nicht oder höchstens sehr diffus enthält. Vertrauen ist aber wieder erforderlich, wenn es darum geht, dass ein Sensor nichts außer dem auszuwertenden Identifikations-Charakteristikum misst.

2.1.1.3 Datenverknüpfung

Besonderes Kennzeichen biometrischer Charakteristika ist ihr hohes Maß an Einmaligkeit. In diesem Sinne lässt sich Biometrie je nach Charakteristikum wie eine Personenkennziffer verwenden. Benutzt man das gleiche biometrische Charakteristikum als Kennung in unterschiedlichen Anwendungen und Datenbanken, wird so eine Verknüpfung der unter dieser Kennung gespeicherten Daten möglich.

Jemand, der Zugriff zu unterschiedlichen Datenbanken bzw. der dazugehörigen Anwendung hat, kann auf diese Weise ein Personenprofil erstellen. Beispiel: Anwendung A ordne einem biometrischen Charakteristikum den Namen einer Person zu und Anwendung B speichere für dasselbe biometrische Charakteristikum ohne weitere persönliche Zusatzinformationen die Ausleihdaten einer biometrisch unterstützten Videothek. Hat nun jemand Zugriff auf beide Anwendungen, kann er unter Umständen dem scheinbar anonymen Videothekenausleiher einen Namen zuordnen. Dies kann z. B. durch direkten Vergleich der gespeicherten biometrischen Referenzdaten (falls diese nicht unterschiedlich verschlüsselt sind) oder durch Anwendung desselben biometrischen Samples mittels einer Testauthentifikation geschehen.

Diese Form der Datenzusammenführung kann in hohem Maße das Recht auf informationelle Selbstbestimmung der betroffenen Personen beeinträchtigen. Deshalb stellt das deutsche Verfassungs- und Datenschutzrecht (anders als etwa skandinavische Länder) sehr hohe Anforderungen an die Verwendung von Charakteristika, die als Allgemeine Personenkennzeichen (PKZ) verwendet werden können.

2.1.1.4 Benutzungszwang

Ein Benutzungszwang ohne Ausweichmöglichkeiten kann gegen das Recht auf informationelle Selbstbestimmung verstoßen. Unabhängig davon verhindert der Benutzungszwang ein natürliches Regulativ, das darin besteht, sich als Betroffener im Falle eines Missbrauchs von einer Anwendung zurückziehen zu können, um damit dem Missbrauch zu entgehen oder den Betreiber zur Systemnachbesserung zu zwingen. In Kundenanwendungen ist das Fehlen von Ausweichlösungen dann weniger kritisch, wenn der Kunde sich nichtbiometrischen Anbietern zuwenden kann oder das Angebot generell nicht lebensnotwendig ist. Ein Authentifikationssystem, das uneingeschränkt alle Betroffenen teilhaben lassen will, muss allerdings schon aus technischen und biologischen Gründen ein Ersatzverfahren (Ausweichlösung) vorsehen, da auf Grund technischer Nichtperfektion (Scanner kann z. B. sehr kleine Finger bei einer Fingerabdruckerkennung nicht auflösen) oder der unzulänglichen Ausprägung eines Charakteristikums (z. B. fehlende Hände im Falle einer Venenmustererkennung) das biometrische System permanent oder temporär scheitern kann.

2.1.1.5 Personen-Überwachung

In den letzten Jahren sind die rechtlichen und die technischen Möglichkeiten für eine legale Überwachung von Personen ständig gestiegen. In der Regel sind unbeteiligte Personen von Überwachungsmaßnahmen mitbetroffen, für die keine Überwachung angeordnet ist.

Mit der Verbesserung der technischen Qualität der Verfahren, der Verkleinerung und Verbilligung der Geräte wächst auch die Gefahr des Missbrauchs von Überwachungstechnik durch Unbefugte. Die Verknüpfung von biometrischen Daten mit Zeit-, Orts- und Verhaltens- oder Kommunikationsdaten ermöglicht eine Überwachung von Personen, z. B. mit Bewegungsprofilen. Die Biometrie kann hierbei eingesetzt werden, um zu verifizieren, dass es sich um die zu überwachende Person handelt. Es besteht aber auch die Möglichkeit, gesuchte Personen beispielsweise auf optischen Medien zu identifizieren, z. B. im Rahmen von Großveranstaltungen. Mit zunehmender Qualität der Verfahren und der Umgebungsvariablen sinkt die Fehlerwahrscheinlichkeit.

2.1.2 Beispiele für den Missbrauch per Identitätsdiebstahl

2.1.2.1 Einkauf unter Nutzung des Fingerabdrucks

Die biometrischen Kundendaten werden erfasst und mit weiteren Kundendaten verknüpft gespeichert. Beim Zahlvorgang wird die Identität allein auf Basis des Fingerabdrucks zentral ermittelt. Auf dieser Basis kann der Betreiber alle Vorgänge registrieren, abrechnen und dem Kunden zur Überprüfung vorlegen. Auf Grund der Orts- und Zeitangaben lassen sich aber auch Plausibilitätsprüfungen vornehmen. Der Betreiber kann mindestens die zweite Transaktion oder gleich das gesamte Kundenkonto sperren oder aber eine weitere Legitimation verlangen, z. B. die Vorlage eines Ausweises.

Möglicher Missbrauch: Mittels einer Kopie des Fingerabdrucks werden verschiedene Käufe getätigt. Der Kunde bemerkt auf seinem Konto unerklärliche Abbuchungen durch den Betreiber des biometrischen Systems. Tatsächlich traten in einem Fall auch nahezu zeitgleich Geldtransfers von weit entfernt liegenden Orten auf. Der Betreiber sperrte sofort das betreffende Kundenkonto, da er zu Recht von einem Identitätsdiebstahl ausging. Aus Kulanzgründen erstattete er alle vom Kunden kritisierten Abbuchungen, obwohl dieser in keinem der Einzelfälle den Identitätsdiebstahl nachweisen konnte. Für den Kunden nachteiliger sind Fälle, wo unbemerkt eine Kopie des Fingerabdrucks erstellt und diese Kopie dann für Bezahlvorgänge eingesetzt wird. Ein Unschuldsnachweis wird möglicherweise schwierig und im Zweifelsfall wird der Kunde den Schaden begleichen müssen.

2.1.2.2 Überwachung von Personen mittels Videokameras

Eine Überwachungskamera dient üblicherweise weniger zum permanenten Identifizieren von Personen, sondern (nach der Prävention) primär zum Identifizieren von Unregelmäßigkeiten und Straftaten. Erst wenn eine Straftat erkennbar ist, besteht auch großes Interesse an der Identifizierung der beteiligten Personen. Hier wird häufig die automatisierte Gesichtserkennung ins Spiel gebracht. Allerdings reicht die Leistung einer Gesichtserkennung oft noch nicht aus, es sind weitere (auch nichtbiometrische) Charakteristika wie Größe, Kleidung etc. zu berücksichtigen. Auch kann es eine große Hilfe für Strafverfolger sein, wenn Verdächtige auf mehreren

Kameras an mehreren Orten zu sehen sind, um einen kompletten Tathergang zur Überführung der Täter zu rekonstruieren.

Missbrauch: Alle Überwachungskameras z. B. einer Stadt oder eines größeren Gebäudekomplexes werden zusammengeschaltet und mit Hilfe einer großen Datenbank von bekannten Gesichtern dazu genutzt, ausgewählte Person an jedem Ort zu erkennen und / oder ein präventives Bewegungsprofil zu erstellen. Anm.: Dieser Missbrauch ist derzeit nur eingeschränkt realisierbar, da die Gesichtserkennung die notwendigen extrem niedrigen Falschakzeptanzraten heute und möglicherweise auch in Zukunft nicht erreichen kann. Teile der hier beschriebenen Methode sind auch in Deutschland in Feldtests untersucht worden und befinden sich u. a. in den USA und Großbritannien bereits im operativen, wenngleich noch fehleranfälligen Einsatz.

2.1.2.3 Missbrauch von Zusatzinformationen in biometrischen Daten

Biometrische Referenzdaten werden von einem Unternehmen ausschließlich in Rahmen der biometrischen Identifikation oder Verifikation verwendet.

Missbrauch durch den Arbeitgeber: Biometrische Referenzdaten werden verwendet, um Hinweise auf mögliche gesundheitliche Beeinträchtigungen oder Risiken zu bekommen. Personalmaßnahmen werden unter Berücksichtigung dieser Informationen vorgenommen, möglicherweise nicht nur aus Informationen, die direkt aus den Daten hervorgehen, sondern auch aus Erkenntnissen mit statistischen Wahrscheinlichkeiten.

Missbrauch durch Versicherungen: Versicherungen können die Gesundheitsinformationen benutzen, um Prämien für Lebens-, Unfall- oder private Krankenversicherungen „kundenindividuell“ zu berechnen oder gar die Versicherungsleistung abzulehnen.

2.2 Wie könnte ein staatlicher Zugriff auf biometrische Daten aussehen?

Ein weiteres Datenschutzrisiko kann für die betroffenen Personen und Träger des biometrischen Charakteristikum darin bestehen, dass die im privaten oder betrieblichen Umfeld gespeicherten Referenzdaten dem Zugriff staatlicher Gefahrenabwehr- oder Strafverfolgungsbehörden unterliegen. Dies kann unberechtigt, aber auch ordnungsgemäß auf gesetzlicher Grundlage geschehen. Letzteres Risiko kann im Prinzip nicht dem Betreiber des biometrischen Systems zugerechnet werden. Er hat aber die Möglichkeit, durch die Wahl einer geeigneten technischen Gestaltung – vor allem durch die ausschließliche Kontrolle der Betroffenen über ihre Daten – den das System nutzenden Personen den Selbstschutz zu ermöglichen und so auch die Akzeptanz des Systems zu erhöhen.

Die genannten Risiken werden insbesondere in Staaten bestehen, die nicht über ein entwickeltes Rechtsstaatssystem verfügen. Aber auch in Deutschland könnten die Behörden auf der Basis bestehender Gesetze (etwa zur Rasterfahndung) auf private biometrische Datenbanken zugreifen. Überdies hat die Entwicklung immer wieder gezeigt, dass neue, zusätzliche Ermächtigungsgrundlagen für den Zugriff auf bestehende Datenbanken geschaffen werden. In beiden Fällen bieten technische Sicherungsinstrumente, die gegen unbefugten Zugriff Dritter schützen sollen, nur bedingt Schutz für die betroffenen Personen, weil die staatlichen Behörden häufig auch die Herausgabe von Passwörtern oder ähnlichen Sicherungsmitteln verlangen können.

Nur wenn die Sicherungen nicht zentral beim Betreiber, sondern lokal (Passwörter oder Token unter ausschließlicher Kontrolle der Nutzer) beim Betroffenen realisiert sind, bestehen die Risiken nicht.

2.3 Sind biometrische Templates unkritischer als biometrische Samples?

Ja. Wenn es darum geht, ggf. vorhandene Zusatzinformationen zu missbrauchen, sind Templates gegenüber Biometrisches Samples eindeutig im Vorteil, vorausgesetzt, der Template-erzeugende biometrische Algorithmus hat diese Zusatzinformationen eliminiert. Es ist allerdings noch für kein System gelungen exakt nachzuweisen, dass ein Template keinerlei Zusatzinformation enthält. Es ist unklar, ob dies überhaupt vollständig möglich ist.

Nein. Wenn der Identitätsdiebstahl mit anschließendem Identitätsmissbrauch das Hauptproblem darstellt, und das dürfte die meisten Missbräuche betreffen, bieten Templates nur eine geringe oder gar keine Verbesserung. Es lässt sich nämlich aus dem Template mit Hilfe mathematischer Methoden unter Nutzung des erzeugenden Erkennungsalgorithmus ein beliebiges neues "biometrisches Sample" rekonstruieren, das der Erkennungsalgorithmus nicht vom original erfassten biometrischen Sample unterscheiden kann. Denn es können zu einer Identität (betroffenen Person) sehr viele biometrische Samples (original erfasste Samples oder auch rekonstruierte Samples) existieren, von denen nicht nur das „richtige" einen Schaden anrichten kann, sondern alle. (Dieses Verfahren funktioniert auch mit verschlüsselten Templates, wenn der Algorithmus Zugriff auf alle notwendigen Schlüssel hat.) Weitere Informationen hierzu finden sich in den Publikationen.

2.4 Sind persönliche Anwendungen völlig unproblematisch?

Nein. Auch persönliche Anwendungen sind so zu schützen, dass ein Identitätsdiebstahl ausgeschlossen ist. Dies betrifft insbesondere nicht-vertrauenswürdige Plattformen wie vernetzte oder physisch zugängliche PCs oder aber mobile Geräte, die man verlieren kann. Man muss damit rechnen, dass berechtigte Mitbenutzer oder Trojanische Pferde Zugriff auf die biometrischen Daten haben, die deshalb unbedingt zu verschlüsseln sind.

3 Schutzmassnahmen

3.1 Welche grundsätzlichen Möglichkeiten des Schutzes vor Missbrauch gibt es?

Folgende Schritte können bei geeigneter Umsetzung einen signifikanten Schutz gewährleisten:

3.1.1 Technische und organisatorische Maßnahmen

- Schutz gegen Diebstahl der biometrischen Daten
- Schutz gegen Einschleusung fremder biometrischer Daten (z. B. durch elektronische Signatur der Referenzdaten)
- Erkennung von Charakteristikumkopien (Plagiat eines Charakteristikums). Dies bezeichnet man auch als Anti-Spoofing. Eine übliche Methode des Anti-Spoofing ist der Einsatz von Lebenderkennung. So wird etwa beim Irisscan die Reaktion der Pupille geprüft, die durch Lichtschwankungen ausgelöst wird. Bei einem als Plagiat präsentiertem Foto eines Auges gibt es keine Pupillenreaktion, die Kopie kann so leicht erkannt werden. Allerdings kann der Einsatz von Lebenderkennung neue Datenschutzrisiken verursachen, beispielsweise wenn auch die für die Lebenderkennung verarbeiteten Daten weitere überschießende Informationen beinhalten. So kann etwa eine verlangsamte Pupillenreaktion auch durch Konsum von Alkohol oder Drogen verursacht sein. Das Sicherheitsziel Überwindungssicherheit des Iris-Sensors und das Datenschutzziel Minimierung von überschießender Information können dann in einem Widerspruch stehen (Dilemma).
- Zugriffs-, Zugangs- und Zutrittskontrolle für alle datenverarbeitenden Systeme und Verbindungen
- Authentizität der Enrolmentdaten: Um die Identität der das biometrische Verfahren Nutzenden beim Enrolment sicherzustellen, muss der Enrolmentprozess unter Hinzuziehung eines Systemverantwortlichen (Zeugen) erfolgen. Dies gewährleistet, dass die abgespeicherten und zu verifizierenden Merkmalsdaten tatsächlich von der enrolten Person stammen und eine Manipulationsmöglichkeit somit minimiert wird.
- Protokolldateien für alle wichtigen Vorgänge und Transaktionen und deren regelmäßige Auswertung
- Regelmäßige Kontrollen und Zertifizierungen über die Funktionsfähigkeit des Systems und die Einhaltung der Vorschriften, möglichst durch unabhängige Institutionen (z. B. Zertifizierungsstellen nach CC, Datenschutzbeauftragte)
- Mitwirkung von Interessenvertretern (z. B. Betriebs- und Personalräten), betrieblichen Datenschutzbeauftragten und Verbänden

3.1.2 Gesetzliche Maßnahmen

- Datenschutzgesetze und -verordnungen
- Abschreckung potentiellen Missbrauchs durch Straftat- und Ordnungswidrigkeitentatbestände

3.1.3 Vertragliche Maßnahmen

- Zusicherung von Maßnahmen, die über die gesetzlichen Mindestanforderungen hinausgehen
- Vertragliche Vereinbarung zur Einhaltung der gesetzlichen Regelungen bei Auftragsdatenverarbeitung

3.2 Wie lassen sich biometrische Referenzdaten vor Diebstahl schützen?

Als wichtigste Schutzmaßnahme ist dafür zu sorgen, dass biometrische Referenzdaten nicht in unberechtigte Hände fallen. Hierfür können klassische organisatorische und technische Datensicherheitsmaßnahmen eingesetzt werden. Je nach Rechtsgrundlage kann der Aufbau eines Datenschutz- und Datensicherheitsmanagements erforderlich sein. Das Datensicherheitsmanagement kann sich an internationalen Standards, wie etwa der Norm ISO 27001, orientieren.

Für biometrische Systeme bestehen die folgenden zusätzlichen Möglichkeiten:

Geschlossene Systeme

Das biometrische System sollte möglichst keine Daten-Verbindung zur Außenwelt (z. B. zum Internet) unterhalten, die es Angreifern ermöglichen könnte, sich über Softwarefehler oder Systemfehlkonfigurationen Zugriff auf die biometrischen Daten zu verschaffen.

Speicherung auf Chipkarten/Token

Die Referenzdaten werden in kryptografisch abgesicherten Smartcard-Chips eines Token gespeichert, so dass sich auch im Falle eines Tokenverlusts ein nichtautorisierter Zugriff wirksam unterbinden lässt.

Verteilte Referenzdaten-Speicherung

Das System speichert in einzelne Teile aufgespaltene Referenzdaten an verschiedenen Orten. Diese Einzelteile sind für sich allein nicht brauchbar und damit nicht missbrauchbar. Eine Zusammenführung erfolgt nur zum Zwecke der Authentifikation. Die Zuordnungstabelle wird ebenfalls separat und verschlüsselt gespeichert.

Hinweis: Vorsicht bei Identifikationssystemen!

Je mehr Referenzdatensätze für eine biometrische Identifikation genutzt werden, desto höher ist naturgemäß die Chance, mit Hilfe eines "namenlosen" Plagiats (d. h. der Charakteristikumskopie einer unbekannten Person) einen Treffer zu erzielen. Deshalb sollten im erfolgreichen Identifikationsfall dem Betroffenen (bzw. dem Fälscher) auf keinen Fall sonstige nichtbiometrische Daten wie z. B. der Namen angezeigt werden (schlechtes Beispiel: "Guten Morgen, Herr Alois Müller!"). Dies könnte

nämlich eine Zuordnung eines "gestohlenen" unbekannten biometrischen Charakteristikums zu einem Betroffenen möglich machen.

3.3 Wie lassen sich gestohlene biometrische Referenzdaten vor Missbrauch schützen?

Für den Fall, dass biometrische Referenzdaten trotz aller Schutzmaßnahmen in falsche Hände geraten, ist es wichtig, durch zusätzliche vorbeugende, technische Maßnahmen dafür gesorgt zu haben, dass der Dieb mit den Referenzdaten nichts anfangen kann. Zu diesen vorbeugenden Maßnahmen, die natürlich nicht alle gleichzeitig realisiert werden müssen, gehören:

3.3.1 Referenzdaten-Verschlüsselung

Der Erkennungsalgorithmus speichert ausschließlich verschlüsselte Referenzdaten, die nur zum Zwecke des Vergleichs temporär entschlüsselt werden. Es gibt verschiedene Verschlüsselungsstufen:

Verschlüsselung mit einem algorithmenspezifischen Schlüssel. Alle Integratoren eines biometrischen Algorithmus (d. h. Applikationsanbieter, die einen fertigen biometrischen Algorithmus in ihre Applikation integrieren) nutzen den gleichen, nur dem Algorithmenanbieter bekannten Schlüssel zur Integration der Biometrie in ihre Anwendung. Nur der Algorithmenanbieter könnte Referenzdaten außerhalb der Erkennungs-Software entschlüsseln.

Verschlüsselung mit einem integratorspezifischen Schlüssel. Alle Produkte eines Algorithmen-Integrators nutzen den gleichen, nur dem Integrator der biometrischen Algorithmen bekannten Schlüssel.

Verschlüsselung mit einem produktspezifischen Schlüssel. Alle Produkte eines Algorithmen-Integrators nutzen einen unterschiedlichen, nur dem Integrator bekannten Schlüssel.

Verschlüsselung mit einem Betroffenen-spezifischen Schlüssel. Jeder Betroffene eines biometrischen Systems hat seinen eigenen, höchstens ihm selbst bekannten aber zumindest nur ihm vollständig unterstellten Schlüssel. In diesem Fall sollte zur Schlüsselspeicherung eine Krypto-Chipkarte genutzt werden. Diese Methode erfüllt auch eine der Forderungen des Datenschutzes, die "technische" Widerrufbarkeit der Einwilligung. Für den Fall des Widerrufs muss der Betroffene lediglich die Chipkarte entwerten.

Zusätzlichen Schutz gewinnt man durch Kombination eines der drei letzten Verfahren mit der ersten Stufe (*Verschlüsselung mit einem algorithmenspezifischen Schlüssel*).

Alternativ zu einer Verschlüsselung der biometrischen Daten mit einem geheimen Schlüssel gibt es auch Verfahren zur Verschlüsselung von auswechselbaren Geheimnissen mit Hilfe des biometrischen Charakteristikum als Schlüssel ("Biometric Encryption"). Da durch Variation des biometrischen Charakteristikums selbst und durch den mit der Erfassung an Sensoren (Messprozess) verbundenen systematischen und zufälligen Fehler das Erkennungssample und das Enrolment-Sample nie identisch sein werden, ist eine Fehlertoleranz erforderlich. Das Verfahren erfordert daher den Einsatz von Fehlerkorrekturmethoden. Allerdings ist noch nicht für alle biometrischen Charakteristika die praktische Einsetzbarkeit und die datenschutz-

technische Überlegenheit dieser Verfahren gegenüber etablierten Methoden erwiesen.

3.3.2 Erschwerung der Personen-Beziehbarkeit

Über Maßnahmen gegen die Korrumpierung des Verschlüsselungs-Schlüssels hinaus kann der Missbrauch gestohlener Referenzdaten dadurch weiter erschwert werden, dass den Referenzdaten keine nichtbiometrischen Daten hinzugefügt werden, die eine direkte Zuordnung ermöglichen. In diesem Fall sind die Referenzdaten nur durch eine laufende Nummer gekennzeichnet, deren Zuordnung zum Betroffenen mit einer an anderem Ort verschlüsselt gespeicherten Tabelle nur durch die Anwendung möglich ist. Sind die Referenzdaten in Dateien gespeichert, sollte auf keinen Fall eine leicht zu ermittelnde Betroffenen-spezifische ID-Nummer als Dateiname gewählt werden. Gestohlene biometrische Charakteristika sind u. U. deutlich schlechter nutzbar, wenn man Ihren Besitzer nicht kennt.

3.3.3 Verzicht auf die Nutzung standardisierter Referenzdaten-Formate

Standardisierte Referenzdaten oder Templates haben den Nachteil, dass sie nicht nur mit einem speziellen Erkennungsalgorithmus zusammenarbeiten, sondern mit allen, die dieses standardisierte Format verstehen. Auf diese Weise werden Angriffe zur Rekonstruktion von Bilddaten aus gestohlenen Referenzdaten erleichtert, siehe Frage zum Thema "Templates versus Samples".

3.3.4 Verzicht auf die Speicherung biometrischer Erfassungs-Samples

Obwohl sich biometrische Samples unter bestimmten Voraussetzungen grundsätzlich auch aus stark komprimierten biometrisches Samples (Templates) rekonstruieren lassen, ist dies doch mit einem gewissen Know-how und Aufwand verbunden. Somit ist auch ein gewisser Schutz gegen schwache Angriffe gewährleistet. Allerdings sinkt mit stärkerer "Komprimierung" der Referenzdaten die Erkennungsleistung.

Gestohlene biometrische Referenzdaten können in der Regel nur dann einen Schaden anrichten bzw. missbraucht werden, wenn das biometrische Zielsystem sich entweder fremde Referenzdaten unterschieben lässt (z. B. durch unberechtigten Systemzugriff und weil das Referenzdatum als digitaler Datensatz nicht signiert wurde) oder wenn es mechanische Kopien nicht von Originalen unterscheiden kann.

3.4 Welche rechtlichen Mittel können dem Schutz biometrischer Daten dienen?

Gesetze und andere Rechtsvorschriften (insbesondere aus dem Bereich des Datenschutz- und Arbeitsrechts) formulieren rechtliche Anforderungen und technische Ziele für die Verarbeitung und Speicherung personenbezogener Daten, zu denen die – als besonders schützenswert eingestuften – biometrischen Daten gehören. Rechtliche Regelungen können zum einen Vorgaben für die Gestaltung technischer Anwendungen enthalten und insoweit direkt dem Schutz der biometrischen Daten und damit der Rechte der Betroffenen dienen. Überdies ergänzen Rechtsnormen technische Schutzmechanismen dort, wo letztere faktisch überwunden werden können oder aus funktionalen Gründen gegenüber bestimmten Personen (etwa Beschäftigten des Betreibers) nicht oder nur eingeschränkt wirksam sind. In diesen Fällen soll

das Datenschutzrecht mit seinen Straf- und Ordnungswidrigkeitenvorschriften einen abschreckenden Effekt haben.

Des Weiteren sollte sich der Betreiber gegenüber den Betroffenen verbindlich verpflichten, geeignete konkrete Schutzmaßnahmen für diese Daten zu ergreifen und ggf. Nutzungseinschränkungen hinzunehmen. Dies kann durch vertragliche Bestimmungen in Form von *Betriebsvereinbarungen* bzw. Einzelvereinbarungen bei Mitarbeiteranwendungen oder in den *Allgemeinen Geschäftsbedingungen* (AGB) bei Kundenanwendungen geschehen. Derartige vertragliche Maßnahmen dienen der differenzierten Beschreibung des zulässigen Umgangs mit den Daten und der Folgen von Fehlverhalten in konkreten Anwendungszusammenhängen. Sie dürfen den generell geltenden gesetzlichen Regeln nicht widersprechen.

Für Mitarbeiteranwendungen wurde von der TeleTrusT e.V. eine *Musterbetriebsvereinbarung* erarbeitet.

Bezüglich der Kundendaten eignen sich AGB in besonderem Maße dazu, Kundenrechte zu fixieren und Zusicherungen zur Anwendung und zum Schutz der biometrischen Daten dem Kunden gegenüber deutlich zu machen.

3.5 Welche vertrauensbildenden Maßnahmen gibt es?

Neben den gesetzlichen Randbedingungen und technischen Schutzvorkehrungen sind *vertrauensbildende Maßnahmen* von besonderer Bedeutung, da sie direkt den Geschäftserfolg beeinflussen können. Soll eine biometrische Anwendung breite Akzeptanz finden, ist neben der Qualität (s. Zertifizierung & unabhängige Überprüfung) des technischen Verfahrens das Vertrauen aller Beteiligten (Betreiber und Betroffene) in die Technik wichtige Voraussetzung. Aus der Sicht der Betroffenen kommt noch die Notwendigkeit des Vertrauens in den Betreiber hinzu. Es gibt eine Reihe von Maßnahmen von Seiten der Hersteller und des Betreibers, die dieses Vertrauen stärken können:

3.5.1 Zertifizierung & unabhängige Überprüfung des Verfahrens

Ein biometrisches System sollte nicht nur unter der Kontrolle eines unabhängigen Datenschutzbeauftragten stehen. Zu empfehlen sind auch Zertifikate nach den Common Criteria (ISO 15408) und Gütesiegel einer unabhängigen Datenschutzorganisation (Beispiel: Datenschutz-Gütesiegel des Landes Schleswig-Holstein). Diese können eingesetzt werden, um die datensicherheits- und datenschutzrechtliche Eignung eines biometrischen Systems nachzuweisen. Für biometrische Systeme existieren im Rahmen der Common Criteria spezielle Prüfkriterien (Biometrics Evaluation Methodology 1.0, BEM). Beispiele für eine derartige Nutzung der Common Criteria stellen die als Referenzen für Systeme geeigneten Schutzprofile (Protection Profiles) für Videoüberwachungsanlagen (PP-0023) und zwei Schutzprofile zur benutzerbestimmbaren Informationsflusskontrolle (PP-0007 und PP-0008). Für biometrische Systeme gibt es u.a. Schutzprofile zur Verifikation (z. B. PP-0016). Die ISO arbeitet derzeit an einer neuen Norm für die Evaluation von biometrischen Systemen (ISO/IEC CD3 19792) unter Datensicherheits- und Datenschutzaspekten.

3.5.2 Transparenz des Verfahrens

Ein nicht zu unterschätzender Beitrag zur Vertrauenswürdigkeit der eingesetzten Technik sind die verfügbaren Informationen seitens des Herstellers. Sie sollten ne-

ben statistischen Fehlerraten (FMR, FNMR, FAR, FRR, etc.) auch Informationen zur Datensicherheit (Sicherheitsfunktionen wie z. B. Zugangskontrolle, Verschlüsselung etc.) und zum Datenschutz (überschießende Informationen in den eingesetzten Referenzdatenformaten, Widerrufbarkeit der Referenzdaten etc.) beinhalten. Sie können durch Prüfberichte und Zertifikate (s. o.) von unabhängigen Dritten bestätigt sein.

Weiterhin relevant ist die Information des Betroffenen durch den Betreiber über die Art und Weise der Nutzung seiner Daten sowie die vorhandenen Schutzvorkehrungen gegen einen eventuellen Daten-Missbrauch durch Dritte.

3.5.3 Freiwilligkeit der Nutzung des Verfahrens

Dem Betroffenen sollte ein nichtdiskriminierendes Ersatzverfahren zur Verfügung stehen, und zwar nicht nur in solchen Fällen, in denen die Biometrie versagt ("Rate der Enrolment-Fehler"). Sie sollte immer auch dann angeboten werden, wenn sich der Betroffene ohne Nennung von Gründen gegen die Nutzung von Biometrie entscheidet. Nichtdiskriminierung bedeutet nicht, dass eine in jeder Beziehung gleichwertige Ersatzlösung gefunden werden muss. Denn ein wichtiger Grund für den Einsatz von Biometrie sind ja gerade ein erhöhter Nutzerkomfort und eine Kostenreduktion.

Biometrische Systeme, die gegen den Willen eines Nutzers eingesetzt werden, haben in aller Regel mit hohen Fehlerraten zu kämpfen. Ob im konkreten Einzelfall mangelnde Kooperation oder ein biologischer Grund vorliegt, ist nicht immer erkennbar.

3.5.4 Selbstbeschränkung des Betreibers

Biometrische Systeme lassen sich vielfältig nutzen und manchmal auch missbrauchen. Um das Vertrauen der Betroffenen zu gewinnen, ist es unerlässlich, dass sich der Betreiber des Systems zu sinnvollen Beschränkungen verpflichtet. Dazu gehören:

- Keine Weitergabe von biometrischen Daten an Dritte
- Keine Auswertung und Speicherung von biometrischen Zusatzinformationen
- Bei Insolvenz und Firmenübernahmen ist sicherzustellen, dass die biometrischen Daten gelöscht werden, wenn der ursprüngliche Zweck der Datenverarbeitung nicht mehr gegeben ist. Bleibt er bestehen (z. B. rechtmäßige Identifizierung von Kunden oder Mitarbeitern), muss keine Löschung erfolgen.
- Eindeutige und bereichsspezifische Zweckbindung der biometrischen Daten
- Überprüfbare Löschung der biometrischen Daten innerhalb festgesetzter Löschfristen.

4 Empfehlungen

4.1 Wie könnte eine datenschutzgerechte Lösung aussehen?

Eine datenschutzgerechte Lösung zeichnet sich durch z. B. folgende Eigenschaften aus:

- Der komplette biometrische Teil der Anwendung, bestehend aus Sensor, Merkmalsextraktion, Referenzdatenspeicher und Merkmalsvergleich, befindet sich in der Verfügungsgewalt des Betroffenen.
- Zweckmäßigerweise ist der biometrische Teil des Systems in einem Token untergebracht, der den Einflussbereich des Betroffenen nicht verlässt.
- Der biometrische Teil des Tokens ist vollständig von der Kommunikationsschnittstelle zum Betreiberteil des Systems abgeschottet.
- Die Kommunikationsschnittstelle ist mit starker Kryptografie geschützt und liefert je nach Anwendung keine oder nur die üblichen Personendaten.
- Die Gültigkeit der verwendeten Zertifikate wird bei jeder Transaktion über oder durch eine vertrauenswürdige dritte Partei (z. B. ein Trustcenter) geprüft. Auf diese Weise lassen sich auch gestohlene Token "deaktivieren".

Mit dem Einsatz eines Token geht allerdings der Vorteil verloren, sich ohne vergessbare oder verlierbare Dinge authentifizieren zu können.

Darüber hinaus sind andere datenschutzgerechte Gestaltungen von biometrischen Systemen mit applikationsspezifischer gesicherter Datenhaltung möglich. Dies ist auch im Einzelfall zu gestalten und zu prüfen.

4.2 Was ist bei Mitarbeiter-Anwendungen zu beachten?

Schon im Vorfeld der Einführung eines biometrischen Systems ist es wichtig, die Mitarbeitervertretung, den betrieblichen Datenschutzbeauftragten und den Sicherheitsbeauftragten nicht nur umfassend zu *informieren*, sondern auch zu *überzeugen*. Dies wird regelmäßig nur bei Wahl eines datenschutzgerechten Systems möglich sein.

Dem Schutz personenbezogener Daten kommt vor allem am Arbeitsplatz eine herausragende Bedeutung zu, weil sich ein Beschäftigter den Risiken für seine informationelle Selbstbestimmung im Arbeitsverhältnis kaum entziehen kann. Die Verwendung personenbezogener Daten bedarf – wie stets – gemäß § 4 Abs. 1 BDSG einer Einwilligung oder normativen Ermächtigung. Als letztere gelten auch Betriebs- oder Dienstvereinbarungen.

In Unternehmen, die dem Betriebsverfassungsgesetz unterliegen, hat der **Betriebsrat** gemäß § 87 Abs. 1 Nr. 1 BetrVG (Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer) und § 87 Abs. 1 Nr. 6 BetrVG (technische Einrichtungen zur Verhaltens- oder Leistungsüberwachung) ein Mitbestimmungsrecht bei der Einführung biometrischer Systeme. Das gilt nach der Rechtsprechung des Bundesarbeitsgerichts auch dann, wenn der Mitarbeiter von biometrischen Systemen im *Betrieb eines Kunden* erfasst wird, den er auf Anweisung seines Arbeitgebers betritt. Nach einem Urteil des Österreichischen Obersten Gerichtshofs gibt es in Österreich sogar eine Reihe von Fällen, in denen eine Weigerung des Betriebsrats nicht über-

wunden werden kann. In Deutschland entscheidet in diesen Fällen (stets) die Einigungsstelle.

Ist das Betriebsverfassungsgesetz nicht anwendbar, kann die Verwendung biometrischer Daten unter Umständen auf § 28 Abs. 1 BDSG gestützt werden, sofern sie der "Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient". Inwieweit derartige technische Kontrollen aber tatsächlich der **"Zweckbestimmung" des Arbeitsvertrages** gelten, ist überaus umstritten und Gegenstand schwieriger Abwägungsprozesse.

Insofern ist die Einigung mit dem Betriebsrat oder – bei dessen Fehlen – mit den Beschäftigten praktisch unverzichtbar. Als Vorbild kann hier die Musterbetriebsvereinbarung des Teletrust e.V. dienen.

5 Entscheidungen von Gerichten und Datenschutzkommissionen

5.1 Mitbestimmung bei Einsatz von Arbeitnehmern in Kundenbetrieb mit Zugangskontrollsystem

Bundesarbeitsgericht, Beschluss vom 27. Januar 2004, 1 ABR 7/03 (Amtliche Sammlung, Band 109, S. 235 ff.)

In diesem Fall hatte ein Unternehmen laufend Wartungsarbeiten in einem Kundenbetrieb durchzuführen, der unter Beteiligung seines Betriebsrats ein Fingerabdrucksystem zur Zugangskontrolle einrichtete und mit dem Wartungsunternehmen vereinbarte, dass auch dessen Arbeitnehmer das System nutzen sollten. Die Arbeitnehmer des Wartungsunternehmens erhielten – ohne Beteiligung ihres eigenen Betriebsrats – eine entsprechende Anweisung. Nach einem ersten, für das Wartungsunternehmen ungünstigen Beschluss des Arbeitsgerichts Frankfurt wurde den Arbeitnehmern der Zugang ohne Nutzung des Systems dadurch ermöglicht, dass sie von Beschäftigten der Kunden durch die Personalschleuse begleitet wurden.

Das Bundesarbeitsgericht beurteilte dies als unzulässig. Eine Mitbestimmungspflichtigkeit bestehe sowohl gemäß § 87 Abs. 1 Nr. 1 Betriebsverfassungsgesetz (BetrVG) (Frage der Ordnung des Betriebs), als auch gemäß § 87 Abs. 1 Nr. 6 BetrVG (Einführung einer technischen Einrichtung zur Verhaltensüberwachung). Der Begriff des Betriebs nach § 87 Abs. 1 Nr. 1 BetrVG sei nicht räumlich, sondern funktional zu verstehen und erfasse deshalb auch außendienstliche Tätigkeiten. Ein im Kundenbetrieb errichteter Betriebsrat könne mangels Mandats und Verhandlungsmöglichkeit die Interessen der auf Grund von Werkverträgen dort tätigen fremden Arbeitnehmer regelmäßig nicht wahrnehmen. Schließlich könne das Wartungsunternehmen nicht einwenden, ihr selbst seien die Verhaltensregeln durch den Kunden vorgegeben. Sie habe vielmehr als Vertragspartner des Kunden die Möglichkeit, darauf Einfluss zu nehmen, unter welchen Bedingungen „ihre“ Arbeitnehmer dort arbeiteten.

5.2 Biometrische Zeiterfassung in einem Krankenhaus (Österreich)

Österreichischer Oberster Gerichtshof, Urteil vom 20. Dezember 2006, 90bA 109/06d

In diesem Sachverhalt gelangte in einem Bezirkskrankenhaus mit 430 Beschäftigten ein Zeiterfassungssystem mittels Fingerabdruckerkennung zum Einsatz. Dabei lag weder die Zustimmung der einzelnen Beschäftigten, noch die des Betriebsrats vor. Der Oberste Gerichtshof bejahte – vergleichbar dem deutschen Bundesarbeitsgericht – die grundsätzliche Mitbestimmungspflichtigkeit und entschied folgerichtig zu Lasten des Krankenhauses. Darüber hinaus beurteilte das Gericht das System auch als „Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer“, die im Sinne von § 96 Abs. 1 Nr. 1 ArbVG „die Menschenwürde berühren“. Das hat – für Österreich – die wichtige Folge, dass die Weigerung des Betriebsrats auch nicht durch eine Entscheidung der Schlichtungsstelle (entspricht der Einigungsstelle im deutschen Recht) überwunden werden kann.

Arbeitgeber in Österreich sind folglich zwingend auf die Zustimmung des Betriebsrats angewiesen, soweit vergleichbare Fälle vorliegen. Entscheidend für den Ausgang des Verfahrens waren drei Faktoren. Zum einen lag die Verfügungsgewalt über die biometrischen Daten ausschließlich beim Arbeitgeber. Darüber hinaus ging es „nur“ um die Arbeitszeiterfassung und nicht etwa um die Sicherheit des Betriebs. Schließ-

lich – und wohl am wichtigsten – hatte der Arbeitgeber die im Rahmen der Verhältnismäßigkeit zu prüfende Erforderlichkeit des Systems nicht dargetan. Nach den Feststellungen des Gerichts war weder ein Vergleich mit anderen bisher verwendeten oder sonst in Frage kommenden Systemen angestellt worden, noch konnte festgestellt werden, dass derartige Verfahren das Ziel der Arbeitszeiterfassung nicht erreichen könnten. Österreichischer Oberster Gerichtshof, Urteil vom 20. Dezember 2006, 90bA 109/06d

In diesem Sachverhalt gelangte in einem Bezirkskrankenhaus mit 430 Beschäftigten ein Zeiterfassungssystem mittels Fingerabdruckerkennung zum Einsatz. Dabei lag weder die Zustimmung der einzelnen Beschäftigten, noch die des Betriebsrats vor. Der Oberste Gerichtshof bejahte – vergleichbar dem deutschen Bundesarbeitsgericht – die grundsätzliche Mitbestimmungspflichtigkeit und entschied folgerichtig zu Lasten des Krankenhauses. Darüber hinaus beurteilte das Gericht das System auch als „Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer“, die im Sinne von § 96 Abs. 1 Nr. 1 ArbVG „die Menschenwürde berühren“. Das hat – für Österreich – die wichtige Folge, dass die Weigerung des Betriebsrats auch nicht durch eine Entscheidung der Schlichtungsstelle (entspricht der Einigungsstelle im deutschen Recht) überwunden werden kann.

Arbeitgeber in Österreich sind folglich zwingend auf die Zustimmung des Betriebsrats angewiesen, soweit vergleichbare Fälle vorliegen. Entscheidend für den Ausgang des Verfahrens waren drei Faktoren. Zum einen lag die Verfügungsgewalt über die biometrischen Daten ausschließlich beim Arbeitgeber. Darüber hinaus ging es „nur“ um die Arbeitszeiterfassung und nicht etwa um die Sicherheit des Betriebs. Schließlich – und wohl am wichtigsten – hatte der Arbeitgeber die im Rahmen der Verhältnismäßigkeit zu prüfende Erforderlichkeit des Systems nicht dargetan. Nach den Feststellungen des Gerichts war weder ein Vergleich mit anderen bisher verwendeten oder sonst in Frage kommenden Systemen angestellt worden, noch konnte festgestellt werden, dass derartige Verfahren das Ziel der Arbeitszeiterfassung nicht erreichen könnten.

5.3 Verarbeitung biometrischer Daten zur Zugangskontrolle (Thermalbad Mondorf, Luxemburg)

Nationale Kommission für den Datenschutz Luxemburg, Beschlüsse im Bereich der Verarbeitung biometrischer Daten zur Zugangskontrolle vom 21. Dezember 2005 und 12.April 2006

Das Thermalbad in Mondorf wollte seinen Clubabonnenten eine Authentifizierung per Fingerabdruck anbieten. Dazu wurde ein System entwickelt, das die Fingerabdrücke aller Abonnenten zentral in einem Rechner verschlüsselt speichert und die Vergleichs-Referenzen mit Hilfe der ID-Nummer eines chipbehafteten Armbands dem Betroffenen zuordnet. Diese Lösung wurde von der Datenschutzkommission mit dem Hinweis auf einen Verstoß gegen die Angemessenheit (Grundsatz der Verhältnismäßigkeit) untersagt.

Erst nachdem der Betreiber sein System so umgestellt hatte, dass die Referenzdaten nicht mehr zentral, sondern individuell auf dem Armbandchip gespeichert wurden, erfolgte Anfang 2006 eine Freigabe durch die Datenschutzkommission.

Glossar

BDSG	Bundesdatenschutzgesetz
Biometrisches Sample	Analoge oder digitale Repräsentation biometrischer Charakteristika
FAR	False Accept Rate (Falsch-Akzeptanz-Rate)
FMR	False Match Rate (Falsch-Übereinstimmung-Rate)
FNMR	False Non Match Rate (Falsch-Nicht-Übereinstimmungs-Rate)
FRR	False Reject Rate (Falsch-Rückweisungs-Rate)
PKZ	Personenkennzeichen
Spoofing	Vortäuschung eines biometrischen Charakteristikums mittels Plagiat
Trojanisches Pferd	siehe Wikipedia
Zutrittskontrolle	nach BDSG Anlage zu §9 Satz 1: Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren Gemäß Grundschutzkatalog des Bundesamtes für die Sicherheit in der Informationstechnik: Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z.B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.
Zugangskontrolle	nach BDSG Anlage zu §9 Satz 1: verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können
Zugriffskontrolle	nach BDSG Anlage zu §9 Satz 1: gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

Quellen

- Albrecht, A. "Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz", Frankfurter Studien zum Datenschutz, Nomos, 2003.
- Aufsichtsbehörden
- BEM - Biometrics Evaluation Methodology (http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf)
- Biometrics in identity management, p. 83-87 (http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.10.biometrics_in_identity_management.pdf)
- Bromba, M. U. A. "On the reconstruction of biometric raw data from template data", 2003-04-20.
- Bromba, M. U. A. "Biometric Myths", 2004-02-28.
- BSI-Seite zur Zertifizierung nach Common Criteria: http://www.bsi.de/zertifiz/index.htm
- BSI-registriertes Schutzprofil PP-0016: http://www.bsi.de/cc/pplist/pplist.htm#officebased
- Bundesarbeitsgericht, "Mitbestimmung bei Einsatz von Arbeitnehmern in Kundenbetrieb mit Zugangskontrollsystem"; Beschluss vom 27.1.2004, 1 ABR 7/03
- Common Criteria: Protection Profiles: http://www.commoncriteriaportal.org/public/expert/index.php?menu=8
- FIDIS-Studie D.6.1 – Forensic Implications on Identity Management Systems (PDF, 9 MB)
- Hammond, P. et al. "3D Analysis of Facial Morphology", (http://www.sq3.org.uk/papers/amjmedgen.pdf)
- Hao, F.; Anderson, R.; Daugman, J.; "Combining Cryptography with Biometrics Effectively", Technical Report, University of Cambridge, 2005. (http://www.cl.cam.ac.uk/users/jgd1000/biokeycrypto.html)
- Hornung, G., Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren; Dissertation, Nomos, 2005.
- Hornung, G., Steidle, R.; Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential, Arbeit und Recht 2005, 201 (http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/aur_2005_06_201-207_hornung_steidle_biometrie.pdf)

- Hornung, G., Biometrische Arbeitszeiterfassung als Beeinträchtigung der Menschenwürde, Arbeit und Recht 2007, 398 (http://www.uni-kas-sel.de/fb7/oeff_recht/publikationen/pubOrdner/2007_Hornung%20AuR_398.pdf)
- ISO/IEC-Normen zur Biometrie: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=true oder http://www.bromba.com/faq/biofaqd.htm#Standards
- ISO/IEC SC37 Standing Document 2, Version 8, Harmonized Biometric Vocabulary, online verfügbar unter: http://www.3dface.org/media/vocabulary.html
- Kindt, E.; Biometric applications and the data protection legislation; DuD • Datenschutz und Datensicherheit 31 (2007) 3
- Landesdatenschutzbeauftragte
- Nationale Kommission für den Datenschutz Luxemburg: "Beschlüsse im Bereich der Verarbeitung biometrischer Daten zur Zugangskontrolle": http://www.cnpd.lu/de/actualites/activite_nationale/2006/04/20_04_2006/index.html
- Urteil des Österreichischen Obersten Gerichtshofs zur biometrischen Zeiterfassung in einem Krankenhaus: http://ris.bka.gv.at/taweb-cgi/taweb?x=d&o=l&v=jus&db=JUST&t=doc4.tmpl&s=(9ObA109/06d)
- TeleTrusT: Kriterienkatalog (http://www.teletrust.de/fileadmin/files/kritkat_2-0.zip)
- TeleTrusT: Orientierungshilfe/Musterbetriebsvereinbarung http://www.teletrust.de/index.php?id=527
- Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/faq/guetesiegel.htm

Links

- Bundesbeauftragter für den Datenschutz: http://www.bfdi.bund.de/
- Virtuelles Datenschutzbüro: http://www.datenschutz.de/
- Verbraucherzentrale - Bundesverband: http://www.vzbv.de/

Mitwirkende

- Heinz Biermann, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Husarenstraße 30, 53117 Bonn
- Manfred Bromba, Bromba GmbH, Geisenhausener Str. 11a, 81379 München
- Prof. Dr. Christoph Busch, Fraunhofer IGD, Fraunhoferstr. 5, 64283 Darmstadt
- Dr. Gerrit Hornung, Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel, Wilhelmshöher Alle 64-66, 34109 Kassel
- Dr. Martin Meints, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstr. 98, 24103 Kiel.
- Dr. Gisela Quiring-Kock, Der Hessische Datenschutzbeauftragte, Gustav-Stresemann-Ring 1, 65189 Wiesbaden

Diese White Paper wurde nach bestem Wissen und Gewissen zusammengestellt. Es erhebt keinen Anspruch auf Fehlerfreiheit, Vollständigkeit oder Aktualität. Dieses Dokument wird weiterentwickelt. Sollten Sie eine Unstimmigkeit feststellen oder Verbesserungsvorschläge haben, wenden Sie sich bitte an info@teletrust.de